(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
1 March 2001 (01.03.2001)

PCT

(10) International Publication Number
WO 01/15381 A1

(51) International Patent Classification[7]: H04L 9/32

(21) International Application Number: PCT/KR00/00924

(22) International Filing Date: 18 August 2000 (18.08.2000)

(25) Filing Language: Korean

(26) Publication Language: English

(30) Priority Data:
1999/34850 21 August 1999 (21.08.1999) KR

(71) Applicant *(for all designated States except US)*: DANAL CO., LTD. [KR/KR]; Samjung Building, 4th floor, 889-75, Daechi-dong, Kangnam-ku, Seoul 135-280 (KR).

(71) Applicant and
(72) Inventor: KIM, Hyeong, Nyeon [KR/KR]; 502-605, Banpomido 2nd Apt., 60-5, Banpo-dong, Seocho-ku, Seoul 137-040 (KR).

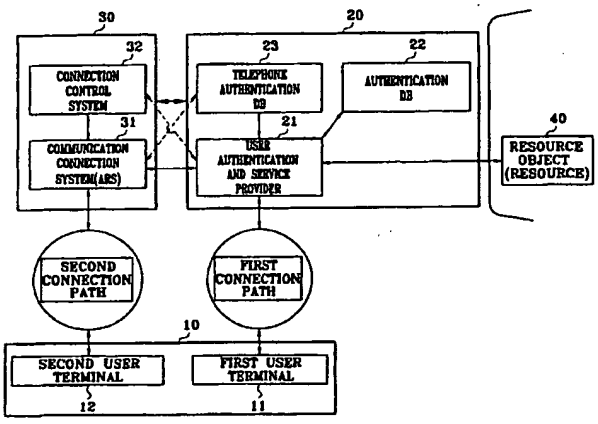
(74) Agent: JO, Eui, Je; Top Patent & Law Firm, Yosam Building, 3F, 648-23, Yuksam-dong, Kangnam-ku, Seoul 135-081 (KR).

(81) Designated States *(national)*: AU, BR, CA, CN, GB, IN, JP, RU, SG, US.

Published:
— *With international search report.*

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

(54) Title: USER AUTHENTICATION SYSTEM USING SECOND CONNECTION PATH



(57) Abstract: A user authentication system using a second connection path, is used for an electronic commerce, an internet stock transaction, a phone banking, in which if a user requests a demand departing from a predetermined range, a user authentication is performed by use of a second connection path. It is preferable that the second connection path is embodied using a telephone network and a communications system. Also, an existing authentication method and an authentication method according to the present invention are organically combined with each other, to perform a user authentication, in which case it is preferable that the authentication via the existing first connection path is applied as a first authentication which allows for a simple connection to the system, and the authentication via the second connection path proposed in the present invention is applied as a final user authentication allowing for an accessing or updating important information departing from the predetermined range. The user authentication system provides reliability and stability much higher than an existing user authentication system, so that a user can transact a comfortable and creditable commerce in an electronic commerce using a communications network, and an effect of promoting a relevant industrial development can be provided.

WO 01/15381 A1

USER AUTHENTICATION SYSTEM USING SECOND CONNECTION PATH

DESCRIPTION

TECHNICAL FIELD

The present invention relates to a user authentication system using a second connection path, and more particularly, to a user authentication system for ensuring reliability and stability much higher than an existing user authentication system, in which a final user authentication is performed via a second connection path such as a telephone communications network different from a first connection path through which a user gains access to a system.

BACKGROUND ART

In general, a user authentication system receives an input identification (ID) and an input password for gaining access to a particular service system, and performs a user authentication with a result obtained by comparing the input ID and password with an ID and a password of a corresponding user which have been stored in advance in the system. Also, to prevent hacking personal credit information or transmission data on a connection path, data such as an ID, password or contents which are transmitted between a user terminal and a service provider system is further encrypted and decrypted or scrambled or descrambled, using a predetermined encryption algorithm.

Meanwhile, according to abrupt development and distribution of the Internet, an electronic commerce, a home banking and a home office work are increasing. Accordingly, a relevant information industry is also under development. To prevent personal credit information and important information from being leaked and damaged by hackers having extremely specialized hacking capability in the information industry, a variety of security systems and user authentication systems are under development. Among them, a password encryption

system has a technological limitation fundamentally. Accordingly, there is no help with respect to a hacking technique of high degree hackers, although a security system such as a firewall has been developed.

In particular, in the case that hackers possessing a high degree hacking technique steal transmission data such as an ID and a password on a connection path, and decrypt the received transmission data, the service provider system cannot help performing a user authentication for an unauthorized user although a perfect firewall exists. Thus, a technological limitation of the existing user authentication system, a gradually intelligent hacking technique, and an increasing hacking possibility stimulate an unstable psychology in connection with utilization of an electronic commerce service of general users. As a result, the relevant industries are not greatly developed.

DISCLOSURE OF INVENTION

To solve the prior art problems, it is an object of the present invention to provide a user authentication system having a remarkably enhanced reliability and stability, in which an interception of user information for authentication by a hacker on a general connection path is prevented, and even though user information for authentication has been intercepted, only an authorized user is assuredly distinguished and authenticated.

To accomplish the above object of the present invention, according to a first aspect of the present invention, there is provided a user authentication system having a first connection path for a user, characterized in that the user authentication system processes a user demand via the first connection path within a predetermined range and performs a user authentication by use of a second connection path, if a demand departing from the predetermined range is requested. It is preferable that the second connection path is embodied using a telephone network and a communications system.

Also, in the case that an existing authentication method and an authentication method according to the present invention is organically

combined with each other, it is preferable that an authentication via the existing first connection path is applied as a first authentication which allows for a connection to the system in order to process a user demand within the predetermined range, and an authentication via the second connection path proposed in the present invention is applied as a final user authentication allowing for an accessing or updating important information departing from the predetermined range. Here, the first and second authentication methods differ distinctively from a simple double authentication method doubly authenticating a user via the same connection path, in the technological configuration and functional effect, which is apparent to a person who has an ordinary skill in the art.

BRIEF DESCRIPTION OF DRAWINGS

The above object and other advantages of the present invention will become more apparent by describing the preferred embodiment thereof in more detail with reference to the accompanying drawings in which:

FIG. 1 is a block diagram showing a user authentication system by use of a second connection path according to a preferred embodiment of the present invention; and

FIG. 2 is a flow-chart view for explaining a user authentication method of the FIG. 1 system.

BEST MODE FOR CARRYING OUT THE INVENTION

Preferred embodiments of the present invention will be described in more detail with reference to the accompanying drawings.

FIG. 1 is a block diagram showing a user authentication system by use of a second connection path according to a preferred embodiment of the present invention. In particular, the user authentication system shown in FIG. 1 illustrates a preferred embodiment of the case that a second authentication scheme using a second connection path, which refers specifically to a telephone communications network, is combined with an existing authentication scheme using a first

connection path. The present invention is not however limited thereto.

The principal configuration of FIG. 1 includes a user interface unit 10 having user terminals 11 and 12 which are individually connected to a respectively different connection path, a service provider system 20 for processing a demand from a user via a first connection path within a predetermined range, and performing a final user authentication by use of a second connection path if a demand departing from the predetermined range is requested, to thereby provide a relevant service, and a communication connect and control system 30, located between the user interface unit 10 and the service provider system 20, for calling up the second user terminal 12 connected to a telephone number of a corresponding user if an authentication of the final user is demanded and transferring user authentication information responsive to the demand of the user authentication information to the service provider system 20. Also, a resource 40 represents a resource object demanding an access of an authorized user or an updating of the user authentication information, in the case that the final user authentication has been performed by a user authentication and service provider unit 21. Here, the resource object demanding the final user authentication corresponds to all objects requiring a user authentication procedure such as a general data file, a DB table, a bank account, and a directory service.

More specifically, the first user terminal 11 in the user interface unit 10 is a user interface connected to the service provider system 20 via the first connection path, for demanding a predetermined service to and from a user. The second user terminal 12 is a user interface connected to the service provider system 20 via the second connection path and the communication connect and control system 30, for inputting the final user authentication information to the systems upon the demand of the service provider system 20 and the communication connect and control system 30. Here, each connection path is realized in various forms according to a service pattern provided from the system. For example, a PSTN (Public Switched Telephone Network), an ISDN (Integrated Services Digital Network), a WAN (Wide Area Network), a LAN (Local Area Network), a mobile radio communications network, or a blue tooth which is a most

likelihood direct communications network is applied as each connection path. Also, each user terminal connected to each connection path is a telephone, a personal computer (PC), an ATM terminal, a mobile phone such as a cellular phone and a PCS, or a terminal incorporated with the Bluetooth for a one-to-one immediate radio communication.

The service provider system 20 includes a user authentication and service provider 21, an authentication database 22 and a telephone authentication database 23 using a telephone network, and provides a service having a different level by a predetermined authentication step. Here, the provided service has a variety of modified service patterns. For example, the service pattern is a predetermined paid service such as an Internet electronic commerce, an Internet mud game service, an Internet audio-on-demand service, an Internet video-on-demand service, and a predetermined program use service. However, the present invention is not limited thereto.

The authentication database 22 stores and manages user IDs and first passwords. A user connects the authentication database 22 to the service provider system 20, via a first user terminal 11 and a first connection path, to use a service within the predetermined range. The authentication database 22 is used to determine whether or not a service use is allowed within a predetermined range. The telephone authentication database 23 stores and manages user Ids, telephone numbers and second passwords. The telephone authentication database 23 is used to finally authenticate whether a corresponding user has an authorized right, if a demand departing from a predetermined range is requested to the system 20. Here, the second password can be pre-set in advance. Also, the second password can be temporarily given by the system or user whenever the final authentication is demanded. Also, the telephone number of a corresponding user can be used as a user ID. Here, a processing departing from a predetermined range in the system means an access to and an updating of important information that should not be disclosed to an illegal user, a paid service, and so on, which go beyond simple inspection of the information. The important information can be a resource object shown in FIG. 1. If an ID of a user and a first

primary password are input from a first user terminal 11 via a first connection path, the user authentication and service provider 21 compares them with those of a corresponding user which are stored in the authentication database 22. As a result, if they match with each other, a user demand is processed within a predetermined range. The user authentication and service provider 21 transfers a telephone number of the corresponding user stored in a telephone authentication database 23 to a communication connection system (ARS) 31, if a demand departing from the predetermined range is requested from a user. The communication connection system 31 dials up a telephone number of the user via a second connection path, connects with the user, receives user authentication information such as a second password, and transfers the received user authentication information to the user authentication and service provider 21. The user authentication and service provider 21 compares the user authentication information, that is, the second password transferred from the communication connection system 31, with those stored in the telephone authentication database 23. As a result, if they match, the user is finally authenticated that the corresponding user has an authorized right, and the relevant service is provided.

The communication connection and control system 30 includes the communication connection system 31 having an ARS processing function basically, and can further include a connection control system 32. The communication connection and control system 30 is installed in the inside of the service provider system 20, or in a communication service company such as a general telephone base station or a mobile communication base station, which is located in the outside of the service provider system 20. The connection control system 32 is a means for checking a final user authentication and connection details of a user for use of the relevant service, and stores and controls telephone number related use details such as a telephone, an inherent number of a second user terminal 12, a number of times of the user inputs, a connection time, a second password for the user who wrongly inputs, to thereby perform a final user authentication, and/or user authentication details related to a predetermined paid service use. By doing so, in the case that an unauthorized user illegally duplicates the

second user terminal 12 to attempt a user authentication, such an illegal duplication and use are traced and the traced result is used as information for billing related to a paid service use.

Further, the user authentication system according to the present invention operates in an application layer which is the highest layer among a network protocol, and operates even in any hierarchical protocols such as TCP/IP, OSI, SNA, DNA and so on, which are used in all communications between respective portions. Also, the user authentication system operates in any encryption technique such as SSL, PCT, KEBEROS and so on in other lower layers and a virtual private network service (VPN). Furthermore, whether or nor a firewall for increasing a security level which can be installed between the respective portions in the whole system, a clustering and a load-balancing executed for a stable operation of a server, a multi-tier via a middle ware are provided, does not influence operation of the user authentication system according to the present invention.

In the user authentication system of FIG. 1 having the above configuration, a preferred method of performing a final user authentication by use of the second connection path will be described with reference to FIG. 2.

Referring to FIG. 2, a user manipulates the first user terminal 11, to gain access to the service provider system 20 via the first connection path at first, and performs a work within an allowable range preset in the service provider system 20 (step 10). Here, the user authentication and service provider 21 compares an ID and a first password of a user input via the first connection path with those of the corresponding user stored in the authentication DB 22, to thereby perform a first user authentication. It is preferable that the first user authentication is used for authenticating a user for a predetermined service that does not require a thorough security. As an example, the first user authentication can be used in the case when the user accesses a home page on the network and inspects known information which is not the important information such as inspection of basic service details, personal particulars and paid services.

If the above system access is primarily allowed, the user authentication and service provider 21 judges whether a user

authentication is needed (step 20). That is, if a user demand via the first connection path does not depart off the predetermined allowable range, a work within the predetermined allowable range can continue. However, if a user demand corresponds to an access to or updating important information departing from the range preset in the system, it is judged that a final user authentication is required.

In step 20, if the final user authentication is demanded, the user authentication and service provider 21 demands that a second password is temporarily input to the first user terminal 11 via the first connection path (step 21). If the second password randomly determined by the user is input to the user authentication and service provider 21 via the first connection path (step 22), the user authentication and service provider 21 stores and controls the input user second password in a record of the corresponding user in the telephone authentication database 23 (step 23).

In the second password establishment process having steps 21 through 23, the second password randomly produced by the user via the first connection path is temporarily stored and controlled, whenever a final user authentication is demanded, to accordingly cause a stronger security level to be enhanced. However, the technological features of the present invention are not limited thereto. That is, the user second password which is stored in the telephone authentication DB 23 for use in final user authentication is preset, and the user second password can be notified to the user randomly. Also, the second password can be received from the user via the second connection path and the second user terminal 12. In addition, the second password can be set identically with the first password, but it is more preferable that the second password is assigned randomly as a security demand level of a site is higher. In particular, the secondary password transferred to the system on the first connection path can be encrypted based on a predetermined algorithm, while the final user authentication system according to the present invention does not need to perform an encryption, which is one of the merits of the present invention. The reason is because confirmation of the second password for the final user authentication is performed via the second connection path and the second user terminal 12 having a user

telephone number stored in the system. Even if a hacker intercepts the second password transferred to the system via the first connection path, the hacker should invade the service provider system 20 and find out a telephone number of the corresponding user. Further, only in the case that the hacker duplicates the second user terminal 12 having the telephone number, or possesses the second user terminal 12 where the telephone number has been set, it is possible to perform an illegal final user authentication.

When the user second password is temporarily set in the telephone authentication DB 23 according to steps 21 through 23, the user authentication and service provider 21 reads out a telephone number of a corresponding user stored in the telephone authentication DB 23 and transfers the read result to the communication connection system 31 (step 24). Accordingly, the communication connection system 31 where an ARS (Automatic Response System) processing is possible calls up the second user terminal 12 via the second connection path by the transferred user telephone number and demands that the user input the second password (step 25). Here, in the case that a user mobile phone number and a user wireless internet phone number are stored in the telephone authentication DB 23, the communication connection system 31 can transfer a message for making the user input the second password, using a SMS (Short Message Service), a WAP (wireless Application Protocol) and a ME (Mobile Explore), as well as the ARS. Particularly, in the case of the wireless Internet phone, the communication connection system 31 can transfer a signal for automatically activating a wireless Internet browser together with the message. Thus, the user can access a wireless Internet server (not shown) to confirm a message, without activating the wireless Internet browser separately.

The user having received the message manipulates the second user terminal 12, and inputs the user second password to the communication connection system 31 via the second connection path (step 26). Here, in the case that the second password stored in the telephone authentication DB 23 has been determined in advance, the second password of the corresponding user is preset in the memory in the second user terminal 12 and the communication connection system

31 reads out the information from the memory automatically, which conveniences the user. Here, the encryption transfer of the user information such as the second password via the second connection path is not essential but optional, as in the first connection path.

The communication connection system 31 transfers the second password input from the second user terminal 12 via the second connection path to the user authentication and service provider 21 (step 27). A connection control system 32 connected to the communication connection system 31 stores and controls the communication details via the telephone number, in which the communication details are used as supervisory trace of illegal users and basic data for billing paid service uses. In more detail, working process related to the communication details and/or user authentication is supervised and recorded by a connection control system 32 for recording security information. The supervised details are taken custody in a database, together with data related to the inherent number of the second user terminal 12, the number of times of inputs, the connection time, the wrongly input second password transferred together with the telephone number automatically from the second user terminal 12, to thereby trace the illegal user in the case that a problem occurs. Also, the database provides a basis on which the service provider charges transaction cost to the telephone number of the customer, in which case the telephone company can make a bill of and receive a product price in addition to the transaction cost, on behalf of the service provider. Thus, to use the above proxy billing and reception method, a separate connection control and account system is constructed in the telephone service provider company (a general telephone base station and a mobile communication base station), and also constructed on the system capable of performing a reliable connection and supervision.

The user authentication and service provider 21 compares the user second password transferred via the second connection path with the user second password stored temporarily via the first connection path (step 28). As a result, if they match with each other, the user connected to the system via the first connection path is authenticated that the user is an authorized user having an authorized right, and thus

the user authentication and service provider 21 provides the corresponding user with a requested service (step 29). As an example, a user who has been authenticated finally in step 29 can be allowed to gain access to the resource object 40 or update the information. Here, the resource object 40 which is accessed or updated according to the final user authentication can be important data related to personal credit card information, bank account, product transaction details, and personal privacy. Meanwhile, in the case that a comparison result tells that they do not match with each other in step 28, the processing is performed according to a particularly determined rule or rolls back an existing transaction of the corresponding user in the system (step 30). Besides, even in the case that a response time from the second user terminal 12 excesses a designated time, a processing can be performed as in step 30.

As described above, the user authentication system using the second connection path according to the present invention performs a user authentication via a connection path different from the first connection path, which is used for service use, to thereby enhance reliability of the user authentication. Further, in the user authentication system using the second connection path according to the present invention, although a hacker intercepts all user information transferred on the two connection paths, the hacker should possess the telephone number of the authorized user and the second user terminal 12 connected to the telephone number. Therefore, a security level and reliability and stability of the user authentication system are remarkably enhanced in comparison with the existing ones.

Also, the user or the service provider system 20 assigns the second password of the authorized user randomly. Accordingly, whenever a user authentication is demanded, a different password is assigned, which makes the second password intercepted by a hacker during user authentication meaningless.

As another preferred embodiment of the present invention, the second user terminal 12 shown in FIG. 1 is embodied with a multi-telephone-number system having at least two telephone numbers. In this case, authentication dedicated telephone numbers of the multi-telephone-number system are stored in the telephone authentication

DB 23. In demanding the user authentication, this method does not respond to the authentication demand in the case that a user authentication is demanded with an inherent number, but connects with the inherent number only when the user authentication is demanded with the authentication dedicated telephone number, to thereby perform an authentication. Therefore, even in the worst case, that is, even in the case that an unauthorized user duplicates the second user terminal 12 having the authorized user inherent telephone number and possesses the duplicated result, the user authentication system according to the present invention connected with the multi-telephone-number system can communicate with a terminal having an inherent number only in the case that another authentication dedicated telephone number, not the inherent number is used as the second connection path for the final user authentication. As a result, the present invention provides the best security system and thus provides a security effect and reliability that is much more remarkably enhanced than the existing technology.

In the case of still another modified embodiment of the present invention, a user iris information or finger print information is used as user authentication information using the second connection path, that is, the second password. In this case, the second user terminal 12 should be embodied as a terminal capable of recognizing the user iris or fingerprint and also the authentication corresponding thereto should be set in the system.

In the case that the user authentication system according to the present invention is applied, an authorized card owner certifies and completes a corresponding transaction, by using a second user terminal 12 such as a mobile phone, even when a cash card or credit card of the user is rent to another person, to thereby enable a creditable transaction, with safe and in comfort.

Meanwhile, a number of modified embodiments which are not referred to are apparent to one having an ordinary skill in the art who understands well the technological concept and the above-described embodiments of the present invention, within the technological scope of the technological concept of the present invention.

INDUSTRIAL APPLICABILITY

As described above, the user authentication system according to the present invention performs a final user authentication via a second connection path different from a first connection path which is used for service utilization, to thereby provide ensure reliability and stability much higher than an existing user authentication system. Also, when the user authentication system according to the present invention is more organically combined with the existing user authentication system, the second password different from the first password for the existing user authentication is used to perform a final user authentication. Accordingly, dangerousness of hacking is minimized to enable a reliable communication transaction. In this case, even if a hacker intercepts a first password, the hacker cannot complete a transaction only in the case that he or she should hold the second user terminal in which the telephone number of an authorized user has been set, to thereby provide a stronger security effect.

Also, in the case that the user authentication system according to the present invention is associated with the multi-telephone-number system and used together, a stability and reliability of the user authentication system can be more remarkably secured.

In the case that the user authentication system according to the present invention is widely distributed and used, reliability and stability of an electronic commerce using a communications network is remarkably secured, to thereby greatly mitigate a sense of unease of a general user, and provide an effect of promoting a relevant industrial development.

CLAIMS

1. A user authentication system having a first connection path for a user, characterized in that said user authentication system processes a user demand via the first connection path within a predetermined range; and performs a user authentication by use of a second connection path, if a demand departing from the predetermined range is requested.

2. The user authentication system of claim 1, wherein said user authentication system comprises:

a service provider system for processing the user demand from a user communication terminal via the first connection path within a predetermined range, and performing a user authentication, if a demand departing from the predetermined range is requested; and

a communication connection and control system for connecting with the user communication terminal via the second connection path according to the user authentication execution of the service provider system, demanding the authentication information for user authentication, and transferring the user authentication information in response to the demanded authentication information to the service provider system.

3. The user authentication system of claim 2, wherein said service provider system comprises:

an authentication database storing data for user authentication;

a user authentication and service provider unit for providing an accessed user via the first connection path with a service, and obtaining authentication information of a corresponding user via the communication connection and control system connected to the second connection path, in the case that the user requests a demand departing from a predetermined range, to thereby perform user authentication; and

a telephone authentication database storing user authentication information via the second connection path.

4. The user authentication system of claim 2, wherein said communication connection and control system comprises a communication connection system connected to the second connection path, for communicating with a user communication terminal connected to the second connection path according to the user authentication execution of the service provider system, to obtain user authentication information and provide the user authentication information to the service provider system.

5. The user authentication system of claim 4, wherein said communication connection and control system further comprises a connection control system for recording and controlling communication details via the second connection path, in order to make a bill of a service use according to the user authentication and a trace of an illegal user.

6. The user authentication system of claim 2, wherein said user communication terminal uses a multi-telephone-number system having at least two telephone numbers, in which the first and second connection paths are assigned and operated with telephone numbers distinctive with each other.

DRAWINGS

FIG. 1

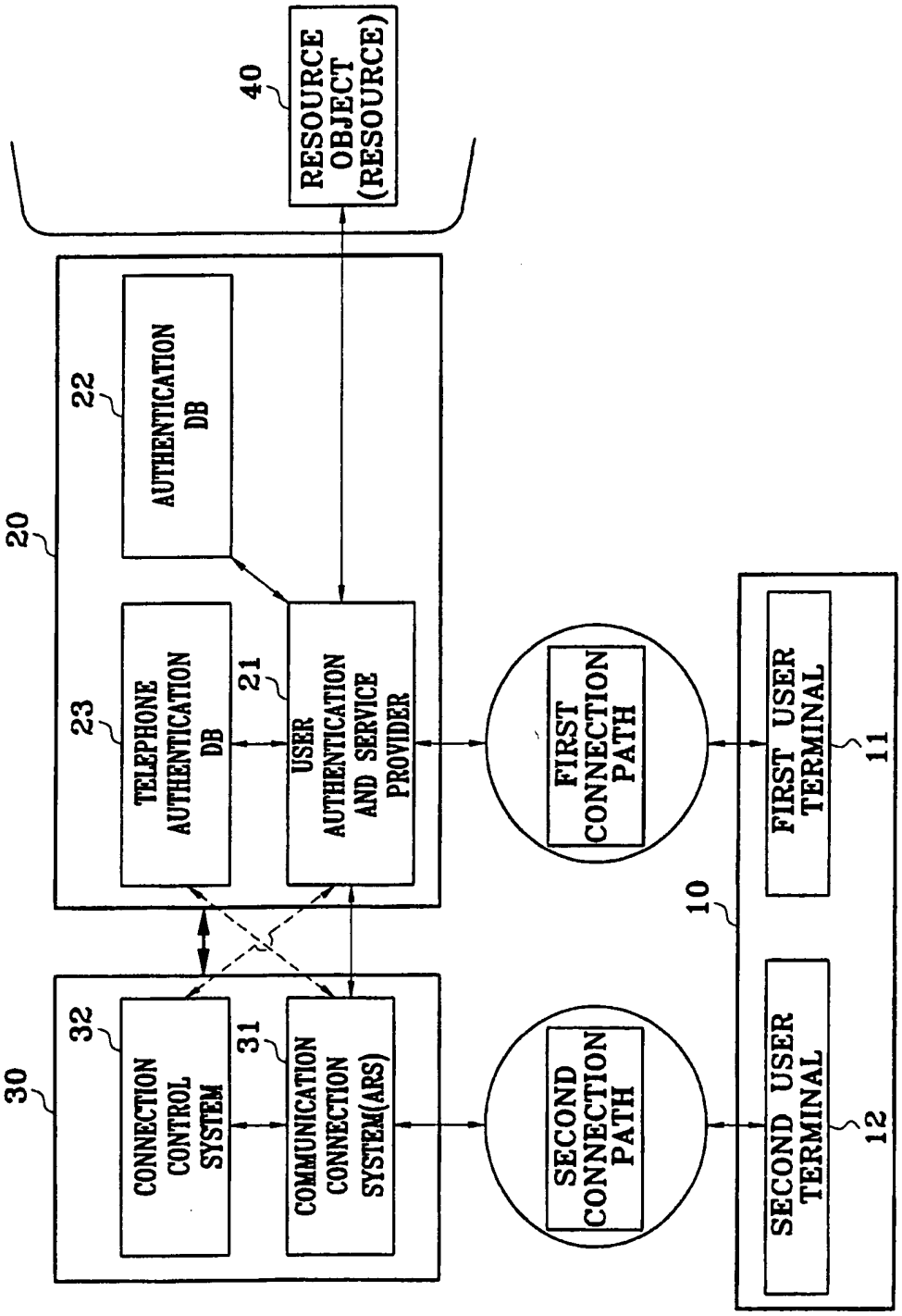
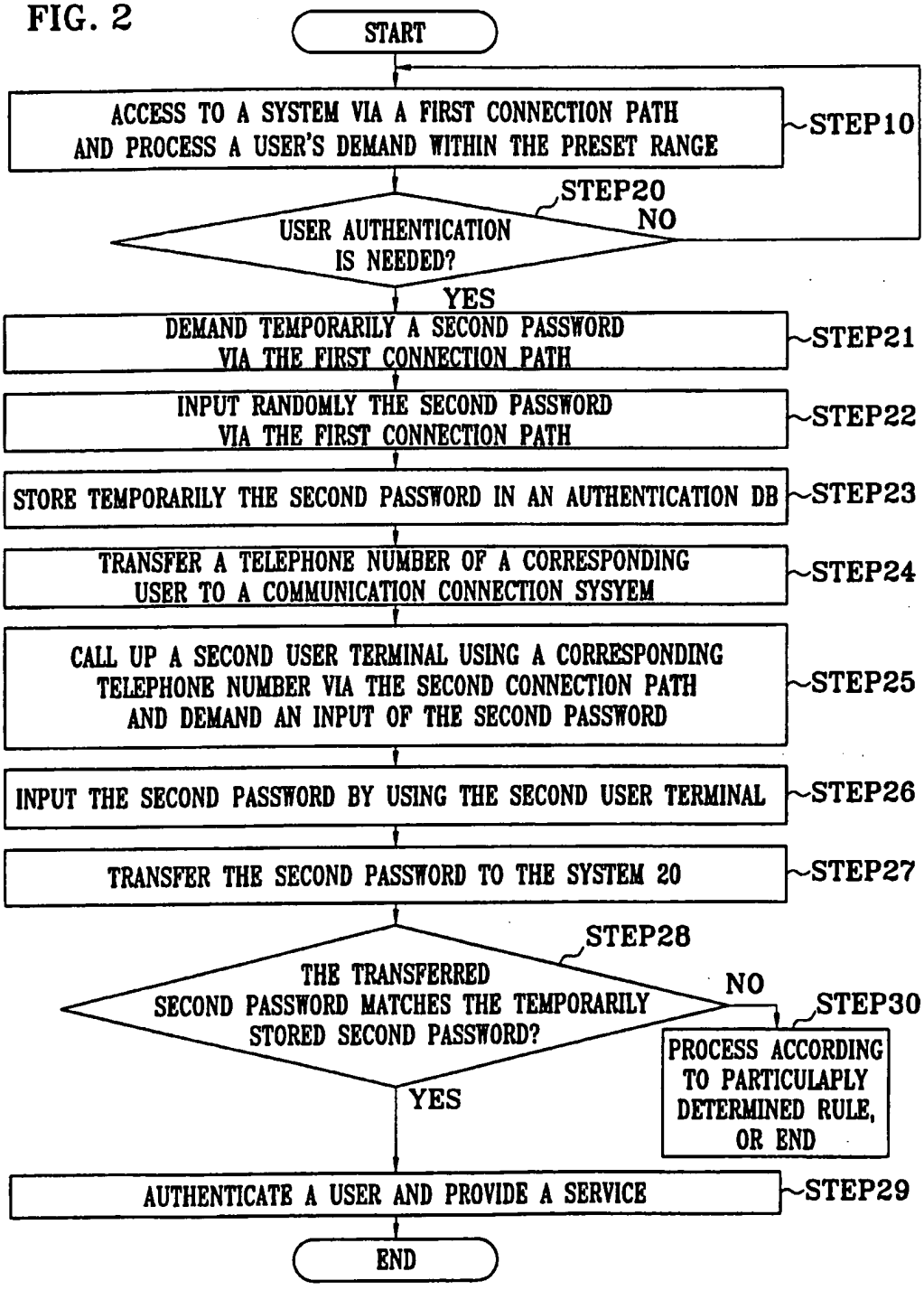


FIG. 2


START
ACCESS TO A SYSTEM VIA A FIRST CONNECTION PATH AND PROCESS A USER'S DEMAND WITHIN THE PRESET RANGE
STEP10
STEP20
USER AUTHENTICATION IS NEEDED?
NO
YES
DEMAND TEMPORARILY A SECOND PASSWORD VIA THE FIRST CONNECTION PATH
STEP21
INPUT RANDOMLY THE SECOND PASSWORD VIA THE FIRST CONNECTION PATH
STEP22
STORE TEMPORARILY THE SECOND PASSWORD IN AN AUTHENTICATION DB
STEP23
TRANSFER A TELEPHONE NUMBER OF A CORRESPONDING USER TO A COMMUNICATION CONNECTION SYSYEM
STEP24
CALL UP A SECOND USER TERMINAL USING A CORRESPONDING TELEPHONE NUMBER VIA THE SECOND CONNECTION PATH AND DEMAND AN INPUT OF THE SECOND PASSWORD
STEP25
INPUT THE SECOND PASSWORD BY USING THE SECOND USER TERMINAL
STEP26
TRANSFER THE SECOND PASSWORD TO THE SYSTEM 20
STEP27
STEP28
THE TRANSFERRED SECOND PASSWORD MATCHES THE TEMPORARILY STORED SECOND PASSWORD?
NO
STEP30
PROCESS ACCORDING TO PARTICULAPLY DETERMINED RULE, OR END
YES
AUTHENTICATE A USER AND PROVIDE A SERVICE
STEP29
END

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR00/00924

A. CLASSIFICATION OF SUBJECT MATTER

IPC7 H04L 9/32

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimun documentation searched (classification system followed by classification symbols)

IPC7 H04L 9/00, 9/32 G06F 17/00

Documentation searched other than minimun documentation to the extent that such documents are included in the fileds searched

KOREAN PATENTS AND APPLICATIONS FOR INVENTIONS SINCE 1983
JAPANESE PATENTS AND APPLICATIONS FOR INVENTIONS

Electronic data base consulted during the intertnational search (name of data base and, where practicable, search trerms used)

WPI

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
P.A P.Y	KR 2000-22713 A(INTERNATIONAL BUSINESS MACHINES CORP.) 25 APRIL 2000 (25.04.2000) page5, lines 4 to 18	1-6 1
P.A P. Y	KR 2000-16713 A(ERICSON INC.) 25 MARCH 2000 (25.03.2000) page 4 , lines 1 to 5, lines 15 to 20	1-6 1
Y	KR 97-126855 B (ELECTRONIC TELECOMMUNICATION RESEARCH INSTITUTE) 17 OCTOBER 1997 (17.10.1997) fig 4, pgae 4 lines 23 to 32	1,2,6
A	KR 99- 45099 A(NIPPON DENKI CORP.) 25 JUNE 1999(25.06.1999) abstract	1-6

[X] Further documents are listed in the continuation of Box C.

[X] See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevence
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevence; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevence; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents,such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 SEPTEMBER 2000 (22.09.2000)	25 SEPTEMBER 2000 (25.09.2000)

Name and mailing address of the ISA/KR
Korean Industrial Property Office
Government Complex-Taejon, Dunsan-dong, So-ku, Taejon
Metropolitan City 302-701, Republic of Korea
Facsimile No. 82-42-472-7140

Authorized officer
LEE, Son Taek
Telephone No. 82-42-481-5667

INTERNATIONAL SEARCH REPORT

International application No.
PCT/KR00/00924

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	KR 98- 144788 B (ELECTRONIC TELECOMMUNICATION RESEARCH INSTITUTE) 23 APRIL 1998 (23.04.1998) page4 lines 11 to 22	1,2,6
P. A	JP 11-289329 A (VEDA RES & AMP; DEV CO.LTD) 19 OCTOBER 1999 (19.10.1999) fig5	1-6
A	EP 436799 A(ALCATEL STK A/S) 10 NOVEMBER 1990 (10.11.1990) fig1, 2	1-6

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/KR00/00924

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
KR 2000-22713 A	25.04.2000	NONE	
KR 2000-16713 A	25.03.2000	NONE	
KR 97-126855 B	17.10.1997	NONE	
KR 99-45099 A	25.06.1999	NONE	
KR 98-144788 B	23.04.1998	NONE	
JP 11-289329 A 12.05.1999	19.10.1999	EP915595 A	
EP 436799 A 19.05.1992 13.09.1991	10.11.1990	US 5115466 A JP 3210847 A	